DCNM から NDFC への移行

前提条件とガイドライン

（注） ファブリック コントローラ サービスで Nexus Dashboard をすでに実行している場合は、このセクションをスキップし、代わりに 既存の ND クラスタをこのリリースへアップグレード の説明に従ってアップグレードしてください。

DCNM 11.5(4) からのアップグレードは、次のワークフローで構成されます。

1. このセクションに記載されている前提条件とガイドラインが満たされていることを確認します。
2. ターゲット NDFC リリースに固有の移行ツールを使用して、既存の設定をバックアップします。
3. ファブリック コントローラ（NDFC）サービスを使用して、新しい Nexus Dashboard クラスタを展開します。

   以前のリリースでは、クラスタがすでに展開された後にサービスをインストールし、有効にする必要がありましたが、このリリースでは、統合インストールの導入により、クラスタの初期展開時にサービスを有効にすることに注意してください。
4. ステップ 1 で作成した設定のバックアップを復元します。

（注） アップグレードに進む前に、各ファブリックのログイン情報を検証します。

これは、 **[Web UI]** > **[管理（Administration）]** > **[ログイン情報の管理（Credentials Manage）]** > **[SAN のログイン情報（SAN Credentials）]**ページで、各ファブリックを選択し、**[検証（Validate）]** を選択して行います。

ペルソナ互換性

適切なアップグレードツールを使用することで、次の表に示すように、ペルソナのために新しく展開された Nexus Dashboard Fabric Controller に、DCNM リリース 11.5(4) からバックアップされたデータを復元できます。

DCNM 11.5（4）からのバックアップ	アップグレード後の NDFC でのペルソナの有効化
OVA/ISO/SE での DCNM 11.5（4）ローカル エリア ネットワーク（LAN）ファブリックの展開	ファブリック コントローラ + ファブリック ビルダー
OVA/ISO/SE でのDCNM 11.5（4）PMN の展開	ファブリック コントローラ +メディアの IP ファブリック（IPFM）
OVA/ISO/SE での DCNM 11.5（4）SAN の展開	SAN コントローラ
Linux での DCNM 11.5（4）SAN の展開	SAN コントローラ
Windows での DCNM 11.5（4）SAN の展開	SAN コントローラ

アップグレード後の機能の互換性

次の表に、アップグレード後に DCNM 11.5(4) のバックアップから復元される機能に関連する注意点を示します。

（注） SAN Insights および VMM Visualizer 機能は、復元後に有効になりません。 Nexus Dashboard ファブリック コントローラ UI の **[設定（Settings）]** > **[機能管理（Feature Management）]** ページで有効にするように選択できます。

DCNM 11.5（4）の機能	アップグレードのサポート
構成された Nexus Dashboard Insights 詳細については、Cisco Nexus Dashboard ユーザー ガイドを参照してください。	サポート対象
コンテナ オーケストレータ (K8s) ビジュアライザ	サポート対象
vCenter による VMM の可視性	サポート対象
構成された Nexus Dashboard Orchestrator	未サポート
設定されたプレビュー フィーチャー	サポート対象外
SAN インストールの LAN スイッチ	サポート対象外
IPv6 で検出されたスイッチ	サポート対象外

DCNM 11.5（4）の機能	アップグレードのサポート
DCNM トラッカー	サポート対象外
ファブリックのバックアップ	未サポート
レポート定義とレポート	未サポート
スイッチのイメージとイメージ管理ポリシー	サポート対象外
SAN CLI テンプレート	11.5(4)から繰り越されません
イメージ/イメージ管理データの切り替え	11.5(4)から繰り越されません
低速ドレイン データ	11.5(4)から繰り越されません
Infoblox 設定	11.5(4)から繰り越されません
エンドポイント ロケーションの設定	アップグレード後に、エンドポイント ロケータ（EPL）を再構成する必要があります。ただし、履歴データは最大 500 MB まで保持されます。
アラーム ポリシーの設定	11.5(4)から繰り越されません
パフォーマンス管理データ	アップグレード後、最大 90 日間の CPU/メモリ/インターフェイス統計情報が復元されます。

既存の DCNM 設定の NDFC への移行

このセクションでは、既存の DCNM 11.5(4) 設定をバックアップし、新しい Nexus Dashboard クラスタを展開し、設定を復元して移行を完了する方法について説明します。

手順

ステップ 1 アップグレード ツールをダウンロードします。

a) NDFC ダウンロードページに移動します。

https://software.cisco.com/download/home/281722751/type/282088134/

b) **[最新のリリース（Latest Releases）]** リストで、ターゲットとするリリースを選択します。

c) 展開タイプに適したアップグレード ツールをダウンロードします。

DCNM 11.5(4) 展開タイプ	アップグレード ツールのファイル名
ISO/OVA	`DCNM_To_NDFC_12_2_1_Upgrade_Tool_OVA_ISO.zip`

DCNM 11.5(4) 展開タイプ	アップグレード ツールのファイル名
Linux または Windows	DCNM_To_NDFC_12_2_1_Upgrade_Tool_LIN_WIN.zip

d) **sysadmin** アカウントを使用して、アップグレード ツール イメージを既存の DCNM 11.5(4) サーバーにコピーします。

ステップ 2 アーカイブを抽出し、Linux/Windows 展開の署名を検証します。

（注） ISO/OVA アーカイブを使用している場合は、次の手順へスキップします。

a) Python 3 がインストールされていることを確認します。

```
$ python3 --version
Python 3.9.6
```

b) ダウンロードしたアーカイブを解凍します。

```
# unzip DCNM_To_NDFC_12_2_1_Upgrade_Tool_LIN_WIN.zip
Archive:  DCNM_To_NDFC_12_2_1_Upgrade_Tool_LIN_WIN.zip
 extracting: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
 extracting: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip.signature
  inflating: ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
  inflating: cisco_x509_verify_release.py3
```

c) 署名を検証します。

ZIP アーカイブ内にはアップグレード ツールと署名ファイルがあります。アップグレード ツールを検証するには、次のコマンドを使用します。

```
# ls -l
total 4624
-rw-rw-r-- 1 root root    1422 Aug 11  2023 ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
-rwxr-xr-x 1 root root   16788 Feb 26 15:57 cisco_x509_verify_release.py3
-rw-r--r-- 1 root root 2344694 Feb 27 07:51 DCNM_To_NDFC_12_2_1_Upgrade_Tool_OVA_ISO.zip
-rwxr-xr-x 1 root root 2359065 Feb  2 09:19 DCNM_To_NDFC_Upgrade_Tool_OVA_ISO
-rw-rw-r-- 1 root root     256 Feb 26 16:54 DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.signature

# ./cisco_x509_verify_release.py3 -e ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM -i
DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip -s DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip.signature -v dgst
 -sha512

Retrieving CA certificate from https://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from https://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM.
Successfully verified the signature of DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip using
ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
```

d) 検証スクリプト署名を確認したら、スクリプト自体を抽出します。

```
# unzip DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
Archive:  DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
   creating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/
  inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/log4j2.properties
  inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/DCNMBackup.sh
  inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/DCNMBackup.bat
   creating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/
  inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/jarchivelib-0.7.1-jar-with-dependencies.jar
```

```
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/bcprov-jdk15on-1.68.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/not-going-to-be-commons-ssl-0.3.20.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/jnm.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/slf4j-simple-1.7.21.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/log4j.properties
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/dcnmbackup.jar
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/sequences.info.oracle
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/tables.info.postgres
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/sequences.info.postgres
inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/tables.info.oracle
```

ステップ 3 アーカイブを抽出し、ISO/OVA 展開の署名を検証します。

（注） Linux/Windows アーカイブを使用している場合は、次の手順にスキップします。

a) ダウンロードしたアーカイブを解凍します。

```
# unzip DCNM_To_NDFC_12_2_1_Upgrade_Tool_OVA_ISO.zip
Archive:  DCNM_To_NDFC_12_2_1_Upgrade_Tool_OVA_ISO.zip
inflating: DCNM_To_NDFC_Upgrade_Tool_OVA_ISO
extracting: DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.signature
inflating: ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
inflating: cisco_x509_verify_release.py3
```

b) 署名を検証します。

ZIP アーカイブ内にはアップグレード ツールと署名ファイルがあります。アップグレード ツールを検証するには、次のコマンドを使用します。

```
$ ./cisco_x509_verify_release.py3 -e ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM -i
DCNM_To_NDFC_Upgrade_Tool_OVA_ISO -s DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.signature -v dgst -sha512

Retrieving CA certificate from https://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from https://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM.
Successfully verified the signature of DCNM_To_NDFC_Upgrade_Tool_OVA_ISO using
ACI_4070389ff0d61fc7fbb8cdfdec0f38f30482c22e.PEM
```

ステップ 4 既存の設定をバックアップします。

バックアップ ツールは、過去 90 日間の Performance Management データを収集します。

a) DCNM リリース 11.5(4) アプライアンス コンソールにログインします。

b) スクリーン セッションを作成します。

次のコマンドは、追加のコマンドを実行するためのセッションを作成します。

```
dcnm# screen
```

このコマンドは、ウィンドウが表示されていない場合、または切断された場合でも実行を続けることに注意してください。

c) スーパー ユーザー（root）アクセス権を取得します。

```
dcnm# su
Enter password: <root-password>
[root@dcnm]#
```

d) OVA および ISO の場合は、アップグレード ツールの実行権限を有効にします。

```
[root@dcnm]# chmod +x ./DCNM_To_NDFC_Upgrade_Tool_OVA_ISO
```

e) 前の手順でダウンロードしたアップグレード ツールを実行します。

- Windowsの場合：

```
G:\DCNM_To_NDFC_Upgrade_Tool_LIN_WIN>DCNMBackup.bat
DCNMBackup.bat
Enter DCNM root directory [C:\Program Files\Cisco Systems\dcm]:

Initializing, please wait...

********************************************************************************

Welcome to DCNM-to-NDFC Upgrade Tool for Linux/Windows.

This tool will analyze this system and determine whether you can move to NDFC 12.2.1 or not.

If upgrade to NDFC 12.2.1 is possible, this tool will create files to be used for performing
 the upgrade.

Thank you!

********************************************************************************

This tool will backup config data. Exporting Operational data like Performance(PM) might
take some time.

Do you want to export operational data also? [y/N]: y
********************************************************************************


Sensitive information will be encrypted using an encryption key.
This encryption key will have to be provided when restoring
the backup file generated by this tool.


Please enter the encryption key:
Enter it again for verification:
….
2024-02-26 17:57:32,247 [main] INFO  DCNMBackup - Creating final tar.gz file....
2024-02-26 17:57:32,649 [main] INFO  DCNMBackup - Final tar.gz elapsed time: 402 in ms
2024-02-26 17:57:32,650 [main] INFO  DCNMBackup - Backup done.
2024-02-26 17:57:32,657 [main] INFO  DCNMBackup - Log file: backup.log
2024-02-26 17:57:32,658 [main] INFO  DCNMBackup - Backup file:
backup11_win57_20240226-172247.tar.gz
```

- Linuxの場合：

```
# ./DCNMBackup.sh
Enter DCNM root directory [/usr/local/cisco/dcm]:

Initializing, please wait...

********************************************************************************

Welcome to DCNM-to-NDFC Upgrade Tool for Linux/Windows.

This tool will analyze this system and determine whether you can move to NDFC 12.2.1 or not.

If upgrade to NDFC 12.2.1 is possible, this tool will create files to be used for performing
 the upgrade.
```

```
Thank you!

********************************************************************************

This tool will backup config data. Exporting Operational data like Performance(PM) might
take some time.

Do you want to export operational data also? [y/N]: y
********************************************************************************


Sensitive information will be encrypted using an encryption key.
This encryption key will have to be provided when restoring
the backup file generated by this tool.


Please enter the encryption key:
Enter it again for verification:
2024-02-27 07:53:46,562 [main] INFO  DCNMBackup - Inside init() method
2024-02-27 07:53:46,564 [main] INFO  DCNMBackup - Loading properties....
2024-02-27 07:53:46,649 [main] INFO  DCNMBackup - Inside checkLANSwitches...
2024-02-27 07:53:46,732 [main] INFO  fms.db - set database url
as:jdbc:postgresql://localhost:5432/dcmdb
2024-02-27 07:53:46,887 [main] INFO  DCNMBackup - LAN Switch count: 0
2024-02-27 07:53:46,889 [main] INFO  DCNMBackup - Inside exportDBTables...
2024-02-27 07:53:46,892 [main] INFO  DCNMBackup - Exporting ---------> statistics
2024-02-27 07:53:46,903 [main] INFO  DCNMBackup - Exporting ---------> sequence
2024-02-27 07:53:46,964 [main] INFO  DCNMBackup - Exporting ---------> clustersequence
2024-02-27 07:53:46,965 [main] INFO  DCNMBackup - Exporting ---------> logicsvr_fabric
……..
2024-02-27 07:53:49,147 [main] INFO  DCNMBackup - Creating final tar.gz file....
2024-02-27 07:53:49,183 [main] INFO  DCNMBackup - Final tar.gz elapsed time: 35 in ms
2024-02-27 07:53:49,183 [main] INFO  DCNMBackup - Backup done.
2024-02-27 07:53:49,183 [main] INFO  DCNMBackup - Log file: backup.log
2024-02-27 07:53:49,183 [main] INFO  DCNMBackup - Backup file:
backup11_onefiveseven.cisco.com_20240227-72149.tar.gz
```

- OVA の場合：

```
# ./DCNM_To_NDFC_Upgrade_Tool_OVA_ISO
********************************************************************************

Welcome to DCNM-to-NDFC Upgrade Tool for OVA/ISO.

This tool will analyze this system and determine whether you can move to
NDFC 12.2.1 or not.

If upgrade to NDFC 12.2.1 is possible, this tool will create files
to be used for performing the upgrade.

NOTE:
Only backup files created by this tool can be used for upgrading,
older backup files created with 'appmgr backup' CAN NOT be used
for upgrading to NDFC 12.2.1

Thank you!

********************************************************************************

Continue? [y/n]: y

Collect operational data (e.g. PM, EPL)? [y/n]: y
```

```
Does this DCNM 11.5(4) have DCNM Tracker feature enabled on any switch on any fabric? [y/n]:
 n

Sensitive information will be encrypted using an encryption key.
This encryption key will have to be provided when restoring
the backup file generated by this tool.

Please enter the encryption key:
Enter it again for verification:

Adding backup header
Collecting DB table data
Collecting DB sequence data
Collecting stored credentials
Collecting Custom Templates
Collecting CC files
Collecting L4-7-service data
Collecting CVisualizer data
Collecting EPL data
Collecting PM data - WARNING: this will take a while!


Collecting AFW app info
Decrypting stored credentials
Adjusting DB tables
Creating backup file
Done.
Backup file: backup11_host108_20240227-153940.tar.gz
```

ステップ 5 このドキュメントの前の章のいずれかの説明に従って、新規に Nexus Dashboard クラスタを展開します。

Nexus Dashboard プラットフォーム、ファブリック コントローラ サービス、および上記の導入の章に記載されている特定のフォーム ファクタのすべてのガイドラインと前提条件を満たしていることを確認します。

（注）
- DCNM 設定の復元に進む前に、Nexus Dashboard ファブリック コントローラ UI で、必要な数の永続 IP アドレスを指定する必要があります。
- 既存の設定で Cisco Smart Software Management（CSSM）に直接接続するスマート ライセンスを使用している場合は、新しい Nexus Dashboard に CSSM Web サイトに到達するために必要なルートがあることを確認する必要があります。

  https://smartreceiver.cisco.com の IP アドレスのサブネットが、Nexus Dashboard 管理ネットワーク用に、Nexus Dashboard の**[管理（Admin）]** > **[システム設定（System Settings）]** > **[ルート（Routes）]** ページのルート テーブルに追加されていることを確認します。

  https://smartreceiver.cisco.com に ping を送信すると、最新のサブネットを見つけることができます。次に例を示します。

```
$ ping smartreceiver.cisco.com
PING smartreceiver.cisco.com (146.112.59.81): 56 data bytes
64 bytes from 146.112.59.81: icmp_seq=0 ttl=52 time=48.661 ms
64 bytes from 146.112.59.81: icmp_seq=1 ttl=52 time=44.730 ms
64 bytes from 146.112.59.81: icmp_seq=2 ttl=52 time=48.188 ms
```

  さらに、NDFC は新しい製品インスタンスと見なされるため、信頼を再確立する必要があります。期限切れの信頼トークンを使用してバックアップを作成した場合は、アップグレード後にスマート ライセンス設定ウィザードを手動で実行し、有効なトークンを入力する必要があります。

ステップ 6 新しいクラスタで設定のバックアップを復元します。

a) admin アカウントで Nexus Dashboard にログインします。
b) 上部のドロップダウンメニューから、**[ファブリック コントローラ（Fabric Controller）]** を選択します。
c) 左のナビゲーション メニューから**[管理（Admin）]** > **[バックアップおよび復元（Backups & Restore）]** を選択します。
d) メイン ペインで、**[復元（Restore）]** をクリックします。
e) **[今すぐ復元（Restore Now）]** ウィンドウで詳細を入力します。
   - 前の手順で作成したバックアップに基づいて、**[設定のみ（Config Only）]** または **[フル（Full）]** を選択します。
   - バックアップ ファイルが保存されている **[ソース（Source）]** を選択し、ファイルをアップロードするか、リモート サーバーの場所とパスを指定します。
   - 設定のバックアップ時に指定した **[暗号キー（Encryption Key）]** を入力します。
   - **[外部サービス IP 設定を無視（Ignore External Service IP Configuration ）]** オプションがオフになっていることを確認します。
f) **[次へ（Next）]** をクリックして情報を確認し、**[復元（Restore）]** で設定を復元します。

   復元の進行中、UI はロックされます。復元に必要な時間は、バックアップ ファイルのデータによって異なります。

復元が正常に完了したら、**[ページのリロード（Reload the page）]** をクリックするか、ブラウザ ページを更新して復元を完了し、Nexus Dashboard ファブリックコントローラの使用を開始します。

ステップ 7 アップグレード後のタスクを完了します。

a) SAN コントローラ ペルソナを使用している場合：

バックアップからデータを復元すると、すべての server-smart ライセンスが **OutofCompliance** になります。

UI の**[操作（Operations）]** > **[ライセンス管理（License Management）]** > **[スマート（Smart）]** ページから、ポリシーを使用したスマート ライセンシングに移行し、SLP を使用して CCSM との信頼を確立できます。

b) ファブリック コントローラ ペルソナを使用している場合：

DCNM 11.5(4) からアップグレードする場合、次の機能については引き継がれないため、再設定が必要です。

- エンドポイント ロケータを再設定する必要があります
- IPAM 統合を再設定する必要があります
- アラーム ポリシーを再設定する必要があります
- カスタム トポロジを再作成して保存する必要があります
- ファブリックで PM 収集を再度有効にする必要があります
- スイッチ イメージをアップロードする必要があります

リリース 11.5(4) の展開タイプ	11.5(4) では、トラップ IP アドレスは以下から収集されます：	LAN デバイス管理の接続性	アップグレード後のトラップ IP アドレス	結果
LAN ファブリック メディア コントローラ	`eth1`（または HA システムの場合 `vip1`）	管理	管理サブネットに属する	Honored 構成の違いは、ありません。対応不要です。

リリース 11.5(4) の展開タイプ	11.5(4) では、トラップ IP アドレスは以下から収集されます：	LAN デバイス管理の接続性	アップグレード後のトラップ IP アドレス	結果
LAN ファブリック メディア コントローラ	eth0（または HA システムの場合 vip0）	管理	管理サブネットに属していない	無視されます。管理プールの別の IP がトラップ IP として使用されます。 構成の違いが作成されます。**Web UI の [LAN]-[Fabrics]-[Fabrics]** で、[Fabric]をダブルクリックして **[Fabric Overview]** を表示します。**[ファブリック アクション（Fabrics Actions）]**ドロップダウン リストから、**[設定の再計算（Recalculate Config）]** を選択します。**[構成の展開（Deploy Config）]** をクリックします。
LAN ファブリック メディア コントローラ	eth0（または HA システムの場合 vip0）	データ	データ サブネットに属する	Honored 構成の違いは、ありません。対応不要です。

リリース 11.5(4) の展開タイプ	11.5(4) では、トラップ IP アドレスは以下から収集されます：	LAN デバイス管理の接続性	アップグレード後のトラップ IP アドレス	結果
LAN ファブリック メディア コントローラ	eth0（または HA システムの場合 vip0）	データ	データ サブネットに属していない	無視されます。データ プールの別のIPがトラップ IP として使用されます 構成の違いが作成されます。**Web UI の [LAN]-[Fabrics]-[Fabrics]** で、[Fabric]をダブルクリックして **[Fabric Overview]** を表示します。**[ファブリック アクション（Fabrics Actions）]**ドロップダウン リストから、**[設定の再計算（Recalculate Config）]** を選択します。**[構成の展開（Deploy Config）]** をクリックします。

リリース 11.5(4) の展開タイプ	11.5(4) では、トラップ IP アドレスは以下から収集されます：	LAN デバイス管理の接続性	アップグレード後のトラップ IP アドレス	結果
SAN 管理	OVA/ISO – • trap.registaddress（設定されている場合） • eth0（trap.registaddress が設定されていない場合） Windows/Linux – • trap.registaddress（設定されている場合） • イベントマネージャ アルゴリズムに基づくインターフェイス（trap.registaddress が設定されていない場合）	N/A	データ サブネットに属する	Honored 構成の違いは、ありません。対応不要です。
		N/A	データ サブネットに属していない	無視されます。データ プールの別のIPがトラップ IP として使用されます

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。